NISTIR 6782

Admission, Discharge, and Transfer System Protection Profile (ADT-PP)

(An ISO.IEC 15408 Security Protection Profile for a Healthcare IT Application System)

Ramaswamy Chandramouli
Glen Marshall

U. S. DEPARTMENT OF COMMERCE
Technology Administration
Computer Security Division
Information Technology Laboratory
National Institute of Standards
and Technology
Gaithersburg, MD 20899

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

NISTIR 6782

Admission, Discharge, and Transfer System Protection Profile (ADT-PP)

(An ISO.IEC 15408 Security Protection Profile for a Healthcare IT Application System)

Ramaswamy Chandramouli
Glen Marshall

U. S. DEPARTMENT OF COMMERCE
Technology Administration
Computer Security Division
Information Technology Laboratory
National Institute of Standards
and Technology
Gaithersburg, MD 20899

March 2002

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Arden L. Bement, Jr., Director

Admission, Discharge and Transfer System Protection Profile (ADT-PP) (An ISO/IEC 15408 Security Protection Profile for a Healthcare IT Application System)

A Proof of Concept Document for Capturing Public Policy Regulatory Requirements into IT Application System Security Requirements

Developed by

Ramaswamy Chandramouli
(National Institute of Standards & Technology)
Glen Marshall
(Siemens Medical Solutions Health Services Corporation)

TABLE OF CONTENTS

SECTION I - PREVIEW

SECTION II (ADMISSIONS DISCHARGE & TRANSFER SYSTEM PROTECTION PROFILE (ADT-PP))

/* This Page is intentionally left blank */

SECTION I
(PREVIEW)

1 INTRODUCTION

The central piece of information in this document is a set of security functional and assurance requirements for an Admissions Discharge and Transfer System (ADT). The ADT is a key information technology (IT) application system used in all major healthcare settings and is the first point of electronic capture of all individually identifiable healthcare information. The set of security functional and assurance requirements is expressed in a format that conforms to the "Protection Profile" framework that is the part of the ISO/IEC 15408 security criteria.

The underlying motivation in developing an ISO/IEC 15408 protection profile for the Admissions, Discharge and Transfer System (hereafter referred to as ADT-PP) is as follows:

"*To illustrate the use of a protection profile as a vehicle for capturing the dictates of public policy regulatory requirements in the form of IT application system security specifications (consisting of both security functional and assurance requirements) for those systems that are used in a healthcare enterprise. Expressing the IT application system's security specifications in a common standardized framework would facilitate the process of interpreting the regulatory requirements among the stakeholders as well as provide a common vocabulary to support subsequent processes like design, development and evaluation of systems. The deployment of such systems in healthcare settings would then serve to meet the underlying goals of the security policy regulation – namely the integrity, availability, confidentiality and privacy of individually identifiable healthcare information.*"

The relevant stakeholders are:

(a) The Healthcare IT system builders or developers
(b) The Healthcare IT system integrators
(c) The Healthcare IT system users
(d) The Healthcare IT system evaluators

The relevant public policy regulatory requirements (that are the focus of this document) are from:

"Security and Electronic Signature Standards; Proposed Rule" that was issued by the Department of Health and Human Services through the Federal Register/Vol. 63, No. 155 dated August 12, 1998, pages 43269 to 43271. The contents of this federal register notification are hereafter referred to as "Proposed HIPAA Security Requirements" in the rest of this document.

2 A BRIEF ON PROPOSED HIPAA SECURITY REQUIREMENTS

The Health Insurance Portability and Accountability Act (HIPAA), (also known as the Kennedy Kassebaum bill), was passed on August 21, 1996. An important section of HIPAA was the one called Administrative Simplification, which called for enactment of standards to " .. reduce the costs and administrative burdens of health care by making possible the standardized, electronic transmission of many administrative and financial transactions that are currently carried out manually on paper."

The Administrative Simplification provisions of HIPAA call for: EDI transaction standards; unique health identifiers for each individual, employer, health plan and healthcare provider; security standards; and, privacy legislation. The logic behind the set of requirements was that standards and unique identifiers would facilitate the exchange of information needed throughout the care delivery system. Making these transactions easier, however, may increase the risk of inappropriate access to sensitive information. Consequently HIPAA also calls for security standards and privacy legislation.

The Health Care Financing Administration (HCFA), in the Department of Health and Human Services, was made responsible for implementing the Administrative Simplification requirements through notice and comment rulemaking. As the first step towards enacting security standards, HCFA issued the "Notice of Proposed Rule Making (NPRM)" through the federal register referred to in the previous section. The proposed HIPAA security requirements apply to claims clearinghouses, health plans, employers and healthcare providers; i.e., "any other person furnishing health care services or supplies" (other than those under the statutory definition of "provider") that maintain or transmit automated health information.

3 ROLE OF ISO/IEC 15408 PPs in HIPAA REQUIREMENTS MAPPING

Many of the proposed HIPAA security requirements apply to the general IT infrastructure in the deploying healthcare enterprise and may not pertain to a specific healthcare IT application system. Hence the first task that is required in the mapping process is to identify the subset of HIPAA security requirements that is relevant for any IT application system in general and to the Admissions, Discharge and Transfer application in particular. Identifying the relevant subset for ADT application system in turn requires us to have an understanding of the functional features of a typical ADT application. We use the word typical here since ADT product offerings from different vendors may have different features and there are different ADT versions for different healthcare settings ranging from clinics to large hospitals. Here our focus is on ADT system for large hospitals. Hence we have to determine a baseline set of features for an ADT system used for large hospitals.

The process of determining a baseline set of functional features for the ADT system and using that as the basis for determining the set of relevant HIPAA security requirements for the system has been demonstrated through a methodology in [1] and is not described in this document. Here we start out from a set of baseline functional

features for the ADT system and the relevant HIPAA security requirements and combine them to describe the security functional requirements (and the associated assurance requirements) as various security services within the framework of an ISO/IEC Protection Profile.

The ISO/IEC 15408 Protection Profile for a healthcare IT application system could be used in the following two ways:

(a) The Methodology described in [1] allocates the various security service requirements expressed in the Protection Profile on the components of the Information System Architecture for a healthcare IT application system to derive a security architecture for the application system. This security architecture will then facilitate the development of HIPAA-compliant healthcare IT application system.

(b) The Protection Profile could be used as the basis for developing the ISO/IEC 15408 Security Target (ST) for the healthcare IT application system. The ST then could form the basis for evaluation/certification of the system for HIPAA compliance since the implementation features claimed in the ST conform to the HIPAA requirements captured in the PP.

4 DOCUMENT ROAD MAP

Section II describes the complete Protection Profile for the Admissions, Discharge and Transfer system (ADT-PP). An illustrative diagram showing the data flows in ADT and associated descriptions (Appendix A) provide the baseline functionality for the system. Appendix B establishes the rationale for the contents of the each of the components of the ADT-PP through mapping tables. Appendix C illustrates the coverage of proposed HIPAA security requirements by the security functional requirements (SFRs) in the ADT-pp. Appendix D contains the bibliography.

/* This Page is intentionally left blank */

SECTION II
(ADMISSIONS, DISCHARGE & TRANSFER SYSTEM PROTECTION PROFILE (ADT-PP))

1 INTRODUCTION

1.1 *IDENTIFICATION*

Protection Profile Title:
Admissions, Discharge and Transfer System Protection Profile (ADT-PP)

Standards Basis:
ISO/IEC 15408 Security Criteria (equivalent Common Criteria 2.1)

Assurance Level:
EAL2 (Augmented)

Registration:
<to be filled in upon registration>

Authors:
Ramaswamy Chandramouli (NIST) and Glen Marshall (MED)

1.2 *BACKGROUND AND MOTIVATION*

The proposed HIPAA security requirements covers the following four areas:
(a) Administrative Procedures
(b) Physical Safeguards
(c) Technical Security Services
(d) Technical Security Mechanisms

Out of the above four categories, the requirements pertaining to Administrative Procedures and Physical Safeguards have to be realized through Management and Operational Controls (vide "Draft HIPAA Security Summit Guidelines – January 12, 2000") defined as part of a Corporate Security Policy. The Technical Security Service requirements have to be realized through security functionality built into IT application systems and the Technical Security Mechanisms have to be realized through a combination of security functionality built into IT application systems as well the IT infrastructure (e.g., LANs and other communication technologies).

The purpose of this protection profile is to capture the HIPAA security requirements pertaining to Technical Security Services and Technical Security Mechanisms as "System Security Functional Requirements" (and associated security assurance requirements) for the "Admissions, Discharge and Transfer System" (hereafter referred to as either ADT or TOE). The use of ADT system for illustrating the use of ISO/IEC 15408 Protection Profile framework for capturing HIPAA security requirements is motivated by the fact

that ADT is the entry-point for practically the entire patient-identifiable information and feeds important subsets of this information category to other related information systems (like the Laboratory and Pharmacy information systems) within the healthcare enterprise.

It must be mentioned that in this proof-of-concept PP, that although the cornerstone of the security policy which drives the Security Functional/Assurance Requirements is based on proposed HIPAA security requirements, other requirements that pertain to the state of security practices in the healthcare industry have also been included as well.

2 TARGET OF EVALUATION (TOE) DESCRIPTION

The point-of-care-ADT software system is designed to perform all functions relating to:

(a) admission,
(b) discharge and
(c) internal transfer (from one bed/room to another, from one hospital service/ward to another or from one status to another (inpatient to outpatient, emergency to inpatient etc))

of patients in a healthcare facility. To facilitate performance of these functions, it should have real-time access to data repositories containing information such as:

(a) Master Patient Indexes
(b) Patient Demographic & Insurance Information
(c) Patient Medical Records (dealing with diagnoses, treatments and allergies) and
(d) Rooms/Bed Support information within a Hospital Service/Nurse Station etc.,

In addition, the information in a point-of-care-ADT system should be accessible from related systems such as:

(a) Orders Application – for entering orders for clinical tests, for ordering medications from pharmacy etc.,
(b) Patient Billing Application – for entering charges, credits and adjustments relating to bed/room services, clinical tests and medications.

Last, but not the least, the information in a point-of-care ADT should be accessible from various report generation tools for generating periodic and ad-hoc reports, for management analysis and control and for meeting local/state/federal regulatory requirements.

A diagram illustrating the nature of data flows between ADT and other related systems in a typical health care enterprise is given in Appendix A.

3 TOE SECURITY ENVIRONMENT

3.1 *ASSUMPTIONS*

This section describes the environmental conditions under which the "Point-of-care_ADT (TOE)" system's resources will be located (physical) , accessed (connectivity) and operated by normal users and administrators (personnel).

3.1.1 Connectivity Assumptions

(a) A.CONNECT – The TOE can only be accessed through designated terminals located in (I) In-Patient Admissions Desk (ii) Out-Patient Admissions Desk and (iii) Emergency Admissions Desk, and other designated points where ADT tasks are performed.

3.1.2 Physical Assumptions

(a) A.RESOURCE_SAFETY – The basic physical resources of TOE (storage devices and processors) are located within a controlled facility that provides a "reasonable amount of safety" from natural hazards and unauthorized physical access.

(b) A.ACCESS_SAFETY – The access resources (terminals, workstations) of TOE are located within areas with restricted access.

3.1.3 Personnel Assumptions

(a) A.USER_TRUST – ADT users can be "reasonably trusted" not to abuse their authorizations and are assumed to have undergone "basic" security awareness training.

(b) A.ADMIN_COMPETENCE - ADT administrators are assumed to be highly trusted, have undergone security awareness training and have the necessary competence to properly specify the security parameters for TOE.

3.2 THREATS

3.2.1 Threats Addressed by TOE's Environment

(a) T.RESOURCE_SECURITY – The basic physical resources of TOE (processors and storage systems) may be subject to natural hazards or damages due to malicious intruders.

(b) T.ACCESS_SECURITY – The devices that provide a) access to TOE (terminals and workstations) and (b) generate outputs from TOE (printers, plotters, etc) may be used by unauthorized personnel.

(c) T.DISCLOSURE – The display device for accessing the TOE as well as the printed outputs from the TOE may be viewed by unauthorized users.

3.2.2 Threats Addressed by TOE

(a) T.ADMIN_DATA_DISCLOSURE – Data supporting security-management functions (like audit trails, authentication, authorization, system configuration, etc) may be viewed by unauthorized users or processes.

(b) T.ADMIN_DATA_CORRUPTION – Data supporting security-management functions may be modified or completely destroyed.

(c) T.CONTROL_SUBVERT – Users may gain direct access to TOE application data by bypassing published interfaces (like application menus) and thereby subvert the usual security controls enforced by TOE.

(d) T.OVERFLOW_ERRORS – The overflow conditions in some of the TOE resources (e.g., audit trails, transaction logs, disk spaces, etc) either may compromise the secure operation of TOE or may result in denial of service.

3.2.3 Threats Addressed jointly by TOE and its environment

(a) T.ADMIN_ERRORS - The administrative functions of TOE may be performed in a manner that compromises the secure operation of the system (e.g., disabling transaction logging or audit process to improve performance, inappropriate audit parameters or system configuration parameters, etc). This threat cannot be entirely addressed by integrity controls on administrative functions incorporated in TOE and hence administrator knowledge, training and integrity also become factors.

(b) T.USER_ERRORS – The secure operation of the TOE may be compromised due to failure of users to follow the guidelines for secure operation. This threat cannot be entirely addressed by TOE integrity controls, so appropriate user training and guidance in secure practices are also issues to be addressed.

3.3 ORGANIZATIONAL SECURITY POLICIES

Information generated, manipulated and used by TOE comes under the category of "Individually Identifiable Health Information" as defined in Section 142.103 of the Federal Register 45 CFR Part 142 (DHHS – Security and Electronic Signature Standards; Proposed Rule). Hence the TOE should be governed by the relevant security policies especially with regard to authentication, access control and audit functions.

(a) P.AUTHENTICATE – The TOE users will be authenticated based upon any two of the following:

- UserIDs and passwords
- UserIDs, passwords, and additional proof such as a smart card of token-ID device
- UserIDs, passwords, and biometric identification

(b) P.ROLES – The TOE will set up roles or groups corresponding to distinct set of organizational roles performed by various users (e.g., Registration Clerk, Staff Nurse, Physician etc.,). Roles may be defined as being partly composed of other roles (e.g., Generic Admission Clerk plus additional functions yields E/R Admission Clerk.).

(c) P.AUTHORIZATION – The set of authorizations (the functions they are allowed to perform in the TOE) for users will be based solely on their membership in an assigned role or group.

(d) P.AUTHORIZED_USE – Data shall only be created, viewed, read, and deleted in accordance with its authorized purposes.

(e) P.AUTHORIZED_TRANSFERS – Data under the control of ADT can only be imported and/or exported from/to other related healthcare IT systems only in accordance with its authorized purposes.

(f) P.AVAILABILITY – Data shall be available to satisfy the ADT business process requirements.

(g) P.INTEGRITY – Data values retain their content integrity.

(h) P.USER_ACCOUNTABILITY – The TOE users must be held individually accountable for all their security-relevant actions.

(i) P.USER_CLEARANCE – Users are cleared for operation of TOE if they have undergone training in the following areas:

(i) Secure Modes of operation (workstation use & Data handling)
(ii) Printer Usage and handling of outputs

(j) P.ADMIN_CLEARANCE – Qualified administrators are cleared for administration of TOE if they have undergone training in the following areas:
(i) Data Backup, Storage & Archiving Procedures
(ii) Data & System Recovery Procedures
(iii) Authentication Data Maintenance (password reuse & change frequency)
(iv) Normal/Emergency Authorization Requests Handling Procedures
(v) Software Upgrades Procedures
(vi) Secure Configuration
and are familiar with the use of associated documentation.

(k) P.ADMIN_ACCOUNTABILITY - The TOE administrators should be held individually accountable for all their administrative actions especially those dealing with authorization grants.

(l) P.PERIODIC_AUDIT – There should be a periodical internal audit review of TOE for conformance to various administrative procedures.

4 SECURITY OBJECTIVES

The Security Objectives are formulated to counter the threats and support the organizational security policies. Since there are threats that are to be addressed entirely by the environment (section 3.1), entirely by TOE (section 3.2) and by a combination of the environment and TOE (section 3.3), the corresponding security objectives also can be classified as those that pertain to: (a) the environment and (b) TOE. Also with respect to organizational security policies, some of the policy requirements can be implemented by building in features in the TOE while some others can only be enforced through the environment.

The environmental measures for addressing threats and/or enforcing policies are generally made up of a combination of physical safeguards and administrative procedures. The environmental security objectives and corresponding threats/policies they address are outlined in section 4.1 while those security objectives that can only be realized through the TOE are given in section 4.2.

4.1 *ENVIRONMENTAL SECURITY OBJECTIVES*

(a) O. RESOURCE_SECURITY – The basic physical resources of TOE must be housed in facilities that conform to the local building codes (in terms of electrical, plumbing, fire safety requirements) and access restricted through human security guards or electronic locks.

(b) O.ACCESS_SECURITY – The devices that provide access to TOE and generate outputs from TOE have to be located in well-designated areas where entry must be restricted to authorized employees of the organization.

(c) O. USER_TRAINING – The TOE users must be provided training in the following areas:

(i) Secure Modes of operation (workstation use & Data handling)
(ii) Printer Usage and handling of outputs

(d) O.ADMIN_TRAINING – The TOE administrators must be provided training in the following areas:
(j) Data Backup, Storage & Archiving Procedures
(ii) Data & System Recovery Procedures

(iii) Authentication Data Maintenance (password reuse & change frequency)
(iv) Authorization Requests Handling Procedures
(v) Software Upgrades Procedures
(vi) Secure Configuration

(e) O.IT_USER_MANUALS – Operational and Training manuals should be developed for areas covered under user training in (c) above. These should be in addition to the user documentation that comes with the TOE.

(f) O. IT_ADMIN_MANUALS – Operational and Training manuals should be developed for areas covered under administrator training in (d) above. These should be in addition to the system administration documentation that comes with the TOE.

(g) O.IT_AUDIT – There should be periodic internal IT audit covering the following areas:
(i) User Training
(ii)Administrator Training
(iii)Conformance to backup, storage, archiving and recovery procedures.
(iv) Sample data audit involving transaction logs & audit trails

4.1 TOE SECURITY OBJECTIVES

(a) O.AUTHENTICATION_SETUP – The TOE should have the capability to support multiple authentication mechanisms, including the quality metrics needed for secrets associated with each type of mechanism, depending upon the "user"/"function performed".

(b) O.ROLE_SETUP – The TOE should provide the capability to define roles, define structural relationships among roles, assign object and functional privileges to roles, assign roles to UserIDs and control the exercise of object and functional privileges by users/administrators by virtue of memberships in roles.

(c) O.PRIV_SCOPE – The set of privileges/authorizations for TOE roles should include: (1) application functions (exercised through menu options) presented by TOE interface and (2) Access Modes for Information Objects under the control of TOE.

(d) O.AUDIT_SETUP – The TOE should provide the capability to capture all security-relevant events in an audit trail. This audit trail should contain, at the minimum, the following fields: (1) the date/time of the event, (2) the user/role that performed the event, (3) the type of the event and, (4) at least one of the following - data viewed/modified by the event or application/administrative function performed in the event.

(e) O.APPLICATION_CONTROLS – The TOE should provide control mechanisms to protect the integrity and confidentiality of stored, imported and exported data and

ensure secure operation of the system. These mechanisms include constraints on exercise of menu options, import of data etc.

(f) O.ADMIN_CONTROLS – The TOE should provide control mechanisms on administrative functions (e.g., session management) so as to protect the integrity of data and functions supporting secure operation of the system (e.g., allowable values for system configuration parameters).

(g) O. ADMIN_DATA_PROTECTION – Data used by TOE for supporting security-relevant functions (authentication data, authorization data, audit data, system configuration data, etc) can only be viewed by authorized TOE administrators. These data will be stored in protected storage volumes and only these authorized administrators shall be allowed to perform maintenance functions on this data (archiving, recovery, etc). Further integrity controls (like triggers) should be set up to prevent accidental or inadvertent deletion/modification of this type of data (e.g., audit trail records generated within a preset threshold period (within the last 30 or 60 days)).

(h) O.OVERFLOW_ALARMS – Thresholds (absolute percentage limits or comparative rate of increase) should be set up for audit trail volumes, transaction log volumes, application data volumes, etc., so that automatic alarms are sent to the administrator for corrective action whenever these volumes exceed the threshold value.

5 TOE SECURITY FUNCTIONAL REQUIREMENTS

5.1 SECURITY AUDIT (FAU)

5.1.1 ADT Security Audit Data Generation (FAU_GEN)

AUDIT DATA GENERATION

5.1.1.1 FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

(a) Start-up and shutdown of the audit functions;
(b) All auditable events for the *basic* level of audit; and
(c) Any other auditable event included by the ST author.

5.1.1.2 FAU_GEN.1.2 (*Refinement*) The TSF shall record within each audit record at least the following information:

(a) Date and time of the event, type of event, subject identity, the userID, the identifier for the role that caused the event, and the outcome (success or failure) of the event; and
(b) For each audit event type, based on the auditable event definition of the functional components included in the PP/ST, *other audit relevant information as deemed appropriate by the ST author.*

USER IDENTITY AND GROUP/ROLE ASSOCIATION

5.1.1.3 FAU_GEN.2.1 **(Refinement)** The TSF shall be able to associate each auditable event with the identity of the user and the role that caused the event.

5.1.2 Security Audit Review (FAU_SAR)

AUDIT REVIEW

5.1.2.1 FAU_SAR.1.1 The TSF shall provide *only the ADT administrative roles and/or individually identified system administrators* with the capability to read *audit records for all events as well as all fields within each record.*

5.1.2.2 FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

RESTRICTED AUDIT REVIEW

5.1.2.3 FAU_SAR.2.1 The TSF shall prohibit all roles read access to the audit records, except for those roles that have been granted explicit read-access.

SELECTABLE AUDIT REVIEW

5.1.2.4 FAU_SAR.3.1 **(Refinement)** The TSF shall provide the ability to perform searches, sorting and ordering of audit data based upon the *following*:

(a) date and time of the event
(b) user **and/or the group/role** that caused the event
(c) type of event, and
(d) success or failure of the event
(e) any other information recorded in the audit record by the ST author in 5.1.2.2

5.1.3 Security audit event selection (FAU_SEL)

SELECTIVE AUDIT

5.1.3.1 FAU_SEL.1.1 **(Refinement)** The TSF shall be able to include or exclude auditable events from the set of audited events based on the *following* attributes:

(a) Object identity, User identity, **Group/Role**, Subject identity, and/or event type
(b) Success or failure of the event
(c) any other information recorded in the audit record by the ST author in 5.1.2.2

5.1.3.2 FAU_SEL.1.1 – ADT.1 **(Extension)** The TSF shall provide only the explicitly authorized administrative groups/roles with the capability to display and select the events to be audited as well as the information that goes into the audit record.

5.1.3.3 FAU_SEL.1.1 – ADT.2 **(Extension)** The TSF shall provide the capability outlined in FAU_SEL.1.1 – ADT.1 to be exercised any time during the operation of the TOE.

5.1.4 Security audit event storage (FAU_STG)

PROTECTED AUDIT TRAIL STORAGE

5.1.4.1 FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

5.1.4.2 FAU_STG.1.2 The TSF shall be able to *prevent and detect* modifications to the audit records.

ACTION IN CASE OF POSSIBLE AUDIT DATA LOSS

5.1.4.3 FAU_STG.3.1 The TSF shall take *the action to notify an identified user or all users belonging to ADT administrative role*, if the audit trail exceeds *a threshold value* (e.g., audit database exceeds a certain disk storage volume, number of audit records exceeds a specified number, audit database size exceeds a certain percentage of the allocated disk volume) that is set by the ST author.

5.2 USER DATA PROTECTION (FDP)

5.2.1 Access Control Policy (FDP_ACC)

5.2.1.1 FDP_ACC.1.1 The TSF shall enforce the [*ADT Access Control SFP*] on the *following subjects*:

(a) ADT User Roles/Groups

5.2.1.2 FDP_ACC.1.1 The TSF shall enforce the [*ADT Access Control SFP*] on the *following objects*:

(a) The application functions (exercised through Menu Options) found on the ADT interface.

(b) Information Objects dealing with Patient-related information (e.g., demographic, insurance, employment etc) and Stay-related information (e.g., room/ward, nurse station etc).

5.2.1.3 FDP_ACC.1.1 The TSF shall enforce the [*ADT Access Control SFP*] on the *following operations involving the subjects and objects*:

(a) Invocation of application functions (in the Menu Option) in ADT interface

(b) Creation, deletion and modification of information objects mentioned in 5.2.1.2 (e.g., creation, deletion and update of one or more records if these information objects are relational database tables).

5.2.1.4 FDP_ACC.1.1 The TSF shall enforce the [*ADT Access Control SFP*] on the *any other subjects, objects and operations included in the ADT Access Control SFP by the ST author.*

5.2.2 ADT Security Attribute based Access Control

5.2.2.1 FDP_ACF.1.1 The TSF shall enforce the [*ADT Access Control SFP*] to objects based on the following:
(a) User Role/Group Memberships
(b) Any other attribute included in the ADT Access Control SFP by the ST author.

5.2.2.2 FDP_ACF.1.2 The TSF shall enforce the *following rules* to determine if an operation among controlled subjects and controlled objects is allowed:
(a) The application functions (in the menu options of the ADT interface) authorized for roles/groups where the user is a member.
(b) The authorizations associated with the information objects mentioned under 5.2.1.2 for the roles/groups.
(c) Any other rule included by the ST author using these authorizations.

5.2.3 Export of ADT data to outside TSF control (FDP_ETC)

EXPORT OF USER DATA WITHOUT SECURITY ATTRIBUTES

5.2.3.1 FDP_ETC.1.1 The TSF shall enforce the [*ADT Access Control SFP*] when exporting user data, controlled under [*ADT Access Control SFP*], to outside of the TSC.

5.2.3.2 FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

5.2.4 Import from outside TSF control (FDP_ITC)

IMPORT OF USER DATA WITHOUT SECURITY ATTRIBUTES

5.2.4.1 FDP_ITC.1.1 The TSF shall enforce the [*ADT Access Control SFP*] when importing user data, controlled under the SFP, from outside of the TSC.

5.2.4.2 FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

5.2.4.3 FDP_ITC.1.3 The TSF shall enforce the *following* rules when importing user data controlled under the SFP from outside the TSC:
(a) Attributes and the associated rules specified by the ST author (examples of attributes are Source Systems from which import is allowed, the timestamps associated with the data etc).

5.2.5 Inter-TSF user data confidentiality transfer protection (FDP_UCT)

BASIC DATA EXCHANGE CONFIDENTIALITY
FDP_UCT.1.1 The TSF shall enforce the [*ADT Access Control SFP*] to be able to *transmit and receive* objects in a manner protected from unauthorized disclosure.

Application Notes: ADT is the focal point for data transfer to a number of other application systems within the healthcare environment like Laboratory Information System, Radiology Information System, Pharmacy System etc. Here the TSF may have to encompass not only the functions that are invoked when the user interacts with the TOE through published interfaces like menus but also operations performed on the ADT data through utilities software like "Bulk Data Transfer Utility".

5.3 *IDENTIFICATION & AUTHENTICATION (FIA)*

5.3.1 Authentication Failure Handling (FIA_AFL)

5.3.1.1 FIA_AFL.1.1 The TSF shall detect when a *specified number of (as specified by ST author)* unsuccessful authentication attempts occur related to *user logging into ADT system.*

5.3.1.2 FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall perform one or more of the following actions:

(a) Issue a suitable warning to the user
(b) Impose a designated duration of black-out period before another authentication attempt can be made.
(c) Any other suitable action considered relevant for the system by ST author.

5.3.2 User Attribute Definition (FIA_ATD)

5.3.2.1 FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users/administrators of ADT system:
(a) User IDs
(b) Group/Role Memberships

5.3.3 Specification of Secrets (FIA_SOS)

5.3.3.1 FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet the quality metrics for the *following types of secrets*:
(a) For Passwords – the minimum length and the type of characters allowed
(b) For Tokens – the minimum length of token keys

5.3.3.2 FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that *contains the quality metrics described in FIA_SOS.1.*

5.3.4 User Authentication (FIA_UAU)

5.3.4.1 FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.3.4.2 FIA_UAU.5.1 The TSF shall provide one or more of the authentication mechanisms from the *following list* to support user authentication:

(a) Passwords
(b) Smart Tokens
(c) Smart Cards

5.3.4.3 FIA_UAU.6.1 The TSF shall re-authenticate the user under the *following conditions*:
(a) After a specified period of inactivity
(b) Upon application-specific conditions specified by the ST author.

5.3.5 User Identification (FIA_UID)

5.3.5.1 FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.4 *SECURITY MANAGEMENT (FMT)*

5.4.1 Management of security functions behavior (FMT_MOF)

5.4.1.1 FMT_MOF.1.1 The TSF shall restrict the ability to *enable and disable* the *following* functions to the *identified set of ADT administrative roles*:
(a) to enable/disable user accounts
(b) to make changes to the list of events to be audited
(c) any other administrative functions identified by the ST author.

5.4.2 Management of Security Attributes (FMT_MSA)

5.4.2.1 FMT_MSA.1.1 The TSF shall enforce the *ADT access control SFP* to restrict the ability to *query, modify and delete* the *following security attributes* to a *set of authorized ADT administrative roles.*
(a) User IDs
(b) User Group/Role Memberships
(c) Any other attribute included in the ADT Access Control SFP by the ST author.

5.4.2.2 FMT_MSA.3.1 The TSF shall enforce the *ADT access control SFP* to provide *restrictive* default values for security attributes that are used to enforce the SFP.

5.4.2.3 FMT_MSA.3.2 The TSF shall allow *authorized ADT administrative roles* to specify alternate initial values to override the default values (for object security attributes) when an object or information is created.

5.4.3 Management of TSF data (FMT_MTD)

5.4.3.1 FMT_MTD.1.1 The TSF shall restrict the ability to *read, modify and delete* the *following TSF data* to *a set of ADT administrative roles*:
(a) Audit records
(b) Any other TSF data specified by the ST author

5.4.4 Time-limited authorization (FMT_SAE)

5.4.4.1 FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for the *following list of security attributes* to *the set of ADT administrative roles.*
(a) User IDs
(b) User Passwords and/or tokens
(c) Any other security attributes specified in the ST by its author

5.4.4.2 FMT_SAE.1.2 For each of the above security attributes, the TSF shall be able to perform the *following actions* after the expiration time for the indicated security attribute has passed.
(a) Inform the user at login time about the expiry of his/her UserID, Password and/or token.
(b) Any other action that is appropriate for other security attribute specified in the ST by its author.

5.4.5 Security Management Roles (FMT_SMR)

5.4.5.1 FMT_SMR.1.1 The TSF shall maintain:
(a) a set of ADT User Roles
(b) *a set of ADT Administrative Roles.*

5.4.5.2 FMT_SMR 1.2 The TSF shall be able to associate users with roles

5.5 *PROTECTION OF TOE SECURITY FUNCTIONS (FPT)*

5.5.1 Time Stamps (FPT_STM)

5.5.1.1 FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.
5.5.1.2 FPT_STM.1.1 – ADT.1 (Extension) The TSF shall use UTC as the timebase.

5.6 *TOE ACCESS (FTA)*

5.6.1 Session Locking (FTA_SSL)

TSF-INITIATED TERMINATION
5.6.1.1 FTA_SSL.3.1 The TSF shall terminate an interactive session after *a specified time interval of user inactivity as specified in the ST by its author.*

5.6.1.2 FTA_SSL.3.1 –ADT.1 (Extension) In an Internet Browser interaction (or similar cases) where session protocol semantics are not defined, any cookies or tokens used to hold state data shall be invalidated and the TSF shall require re-authentication per 5.3.4.3 (FIA_UAU.6.1)

5.7 TRUSTED PATHS/CHANNELS (FTP)

5.7.1 Inter-TSF trusted channel (FTP_ITC)

5.7.1.1 FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

5.7.1.2 FTP_ITC.1.2 The TSF shall permit *the remote trusted IT product* to initiate communication via the trusted channel.

5.7.1.3 FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *the following functions:*

(a) Importing data from ADT to other healthcare systems like Laboratory Information System, Radiology Information System, Billing System etc.,

(b) Any other function (which the ST author considers appropriate) for which a trusted channel is required.

6 TOE SECURITY ASSURANCE REQUIREMENTS

6.1 CONFIGURATION MANAGEMENT (ACM)

6.1.1 CM Capabilities (ACM_CAP)

CONFIGURATION ITEMS

6.1.1.1 ACM_CAP.2.1C The reference for the TOE shall be unique to each version of TOE

6.1.1.2 ACM_CAP.2.2C The TOE shall be labeled with its reference

6.1.1.3 ACM_CAP.2.3C The CM documentation shall include a configuration list

6.1.1.4 ACM_CAP.2.4C The configuration list shall describe the configuration items that comprise the TOE.

6.1.1.5 ACM_CAP.2.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

6.1.1.6 ACM_CAP.2.6C The CM system shall uniquely identify all configuration items.

6.2 DELIVERY AND OPERATION (ADO)

6.2.1 Delivery (ADO_DEL)

6.2.1.1 The ADT documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user' site.

6.2.2 Installation, Generation, and Start-up (ADO_IGS)

6.2.2.1 ADO_IGS.1.1C The ADT documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

6.3 DEVELOPMENT (ADV)

6.3.1 Functional Specification (ADV_FSP)

INFORMAL FUNCTIONAL SPECIFICATION

6.3.1.1 ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.
6.3.1.2 ADV_FSP.1.2C The functional specification shall be internally consistent.
6.3.1.3 ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
6.3.1.4 ADV_FSP.1.4C The functional specification shall completely represent the TSF.

6.3.2 High-level design (ADV_HLD)

DESCRIPTIVE HIGH-LEVEL DESIGN

6.3.2.1 ADV_HLD.1.1C The presentation of the high-level design shall be informal.
6.3.2.2 ADV_HLD.1.2C The high-level design shall be internally consistent.
6.3.2.3 ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.
6.3.2.4 ADV_HLD.1.4C The high-level shall describe the security functionality provided by each subsystem of the TSF.
6.3.2.5 ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
6.3.2.6 ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.
6.3.2.7 ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

6.3.3 Representation correspondence (ADV_RCR)

INFORMAL CORRESPONDENCE DEMONSTRATION

6.3.3.1 ADV_RCR.1.1C (refined): The developer of the TOE shall provide an analysis of correspondence between the following adjacent pairs of TSF representation for ADT: High-level design and Functional specification. If ST is also provided, then the correspondence should include the following pairs as well: (a) High-level design and TOE summary specification and (b) TOE summary specification and Functional specification. The analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

6.4 GUIDANCE DOCUMENTS (AGD)

6.4.1 Administrator guidance (AGD_ADM)

6.4.1.1 ADV_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
6.4.1.2 ADV_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.
6.4.1.3 ADV_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
6.4.1.4 AGD_ADM.1.4C The administrator shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.
6.4.1.5 AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
6.4.1.6 AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
6.4.1.7 AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.
6.4.1.8 AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

6.4.2 User guidance (AGD_USR)

6.4.2.1 AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
6.4.2.2 AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

6.4.2.3 AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
6.4.2.4 AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.
6.4.2.5 AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.
6.4.2.6 AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

6.5 TESTS (ATE)

6.5.1 Coverage (ATE_COV)

EVIDENCE OF COVERAGE

6.5.1.1 ATE_COV.1.1C The evidence of test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

6.5.2 Functional Test (ATE_FUN)

6.5.2.1 ATE_FUN.1.1C The test documentation shall consists of test plans, test procedure descriptions, expected test results and actual test results.
6.5.2.2 ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
6.5.2.3 ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
6.5.2.4 ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.
6.5.2.5 ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

6.5.3 Independent Testing (ATE_IND)

INDEPENDENT TESTING – SAMPLE

6.5.3.1 ATE_IND.2.1C The TOE shall be suitable for testing.
6.5.3.2 ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

6.6 VULNERABILITY ASSESSMENT (AVA)

6.6.1 Strength of TOE security functions (AVA_SOF)

6.6.1.1 AVA_SOF.1.1C For each mechanism with strength of security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

6.6.1.2 AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

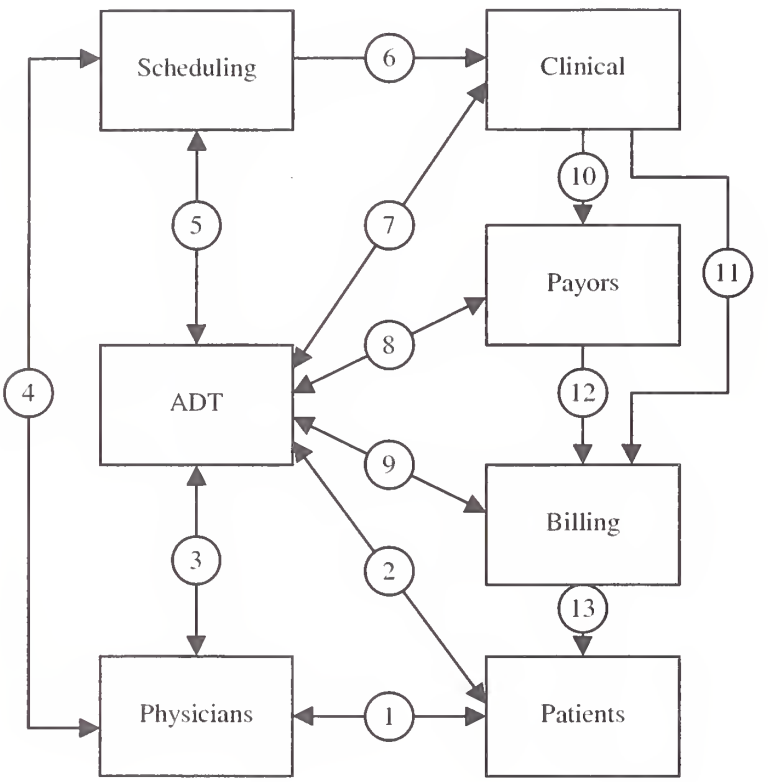
6.6.2 Vulnerability Analysis (AVA_VLA)

DEVELOPER VULNERABILITY ANALYSIS

6.6.2.1 AVA_VLA.1.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Appendix A
Illustrative Diagram for ADT Data Flows

The following diagram illustrates the nature of data flows with the ADT system and other systems with which it communicates. This is to illustrate the central nature of ADT applications for healthcare and their importance to privacy. It is not a data model nor a complete enumeration of all ADT data flows.



1. Patient-Physician

   This interaction is key in the managed care model, which is widely employed. The patient provides identification, permission, health status, and financial data to the physician. The physician provides healthcare and billing data to the patient.

2. Patient-ADT

   The patient provides identification, permission, health status, and financial data to ADT. ADT provides healthcare and billing data to the patient.

3. Physician-ADT

   The physician provides patient identification, treatment referral, and care-authorization data to ADT. ADT provides confirmation and patient-identifiable census data to the physician.

4. Physician-Scheduling

   The physician provides patient identification, treatment referral, and care-authorization data to scheduling. ADT provides patient-identifiable treatment referral and scheduling data to the physician.

5. ADT-Scheduling

   The Scheduling system provides patient identification, treatment referral, and care-authorization data to ADT. ADT provides patient-identifiable schedule confirmation data to Scheduling.

6. Scheduling-Clinical

   The Scheduling system provides patient identification, treatment referral, and care-authorization data to Clinical departments.

7. ADT-Clinical

   ADT provides patient identification, treatment referral, and care-authorization data to Clinical departments. Clinical departments may provide patient-identifiable workflow status information to ADT.

8. ADT-Payors

   ADT provides patient identification, treatment referral, and care-authorization data to Payors. Payors provide patient-identifiable financial information (e.g., insurance coverage) to ADT.

9. ADT-Billing

   ADT provides patient identification and financial information to Billing. Billing provides patient financial data to ADT, e.g., demographics and account status from prior visits.

10. Clinical-Payor

    Clinical systems provide patient-identifiable health status data to payors

11. Clinical-Billing

    Clinical systems provide patient-identifiable health status and event-completion data to Billing, which adds it to the patient's bill to establish financial obligation of the payor and/or patient.

12. Payor-Billing

    The Billing system provides patient-identifiable health status and accumulated treatment data to Payors. Payors provide patient-identifiable payment data to Billing.

13. Patient-Billing

    The Billing system provides patient-identifiable health status and accumulated treatment data to Patients. Patients provide patient-identifiable payment data to Billing.

Appendix B

The purpose of the rationale material is to show that the content of the ADT-PP document truly captures the security functional and assurance requirements for an admissions discharge and transfer system taking into account the operational and regulatory environment in which such a system is being deployed. This is accomplished by providing suitable justifications for the choice of each of the line items in "security objectives" and "security functional requirements" categories as well for the choice of the overall "security assurance level" for the ADT system.

B.1 Security Objectives Rationale

This section lists each of the security objectives in section 2, provides a justification for its inclusion in the ADT-PP and correlates it with the threat(s) it is meant to counter and the policy component(s) it is meant to support as well the relevant security usage assumption. Table B.1.1 deals with environmental security objectives and table B.1.2 deals with TOE security objectives.

Environmental Security Objective	**Threat Addressed**	**Policy Supported**	**Usage Assumption**
O.RESOURCE_SECURITY - protects against malicious intruders and minimizes the risk of natural hazards.	T.RESOURCE_ SECURITY		A.RESOURCE_ SAFETY
O.ACCESS_SECURITY - restricts access to locations where resources that interact with TOE are located.	T.ACCESS_ SECURITY		A.ACCESS_ SAFETY, A.CONNECT
O.USER_TRAINING & O.IT_USER_MANUALS - minimizes risk due to benign users compromising the security of the system due to lack of knowledge of safe operating procedures.	T.DISCLOSURE, T.USER_ERRORS (partial),	P.USER_ CLEARANCE, P.AUTHORISED_USE (partial), P.AUTHORIZED_TRANSFERS (partial)	A.USER_ TRUST
O.ADMIN_TRAINING & O.IT_ADMIN_MANUALS - Training in specific security-relevant operational areas minimizes the risk of admin errors.	T.ADMIN_ ERRORS (partial)	P.ADMIN_ CLEARANCE P.AVAILABILITY (partial)	A.ADMIN_ COMPETENCE
O.IT_AUDIT - ensures that operational and training needs are met in practice.		P.PERIODIC_ AUDIT	

Table B.1.1: Correlating environmental security objectives to threats, policies and usage assumptions

TOE Security Objective	Threat Addressed	Policy Supported	Usage Assumption
O.AUTHENTICATION_SETUP - Users have varying degrees of access to TOE resources and more the criticality of function performed, stronger should be the authentication.		P.AUTHENTICATE	
O.ROLE_SETUP - For effective control of privileges, user/administrator access to privileges should be mediated through roles.		P.ROLES, P.AUTHORIZATION, P.AUTHORIZED_USE (partial), P.AUTHORIZED_TRANSFERS (partial)	
O.PRIV_SCOPE - privileges should only pertain to and can only be exercised through designated TOE interfaces like application menus etc.,	T.CONTROL_SUBVERT		
O.AUDIT_SETUP - all security-relevant actions should be traceable to the person who performed them.		P.USER_ACCOUNTABILITY, P.ADMIN_ACCOUNTABILITY	
O.APPLICATION_CONTROLS - The set of user actions on TOE are constrained through application-level controls.	T.USER_ERRORS (partial)	P.INTEGRITY, P.AUTHORIZED_USE (partial), P.AUTHORIZED_TRANSFERS (partial)	
O.ADMIN_DATA_PROTECTION - higher degree of protection is needed for data that forms the basis of secure operation of TOE as compared to application data.	T.ADMIN_DATA_DISCLOSURE, T.ADMIN_DATA_CORRUPTION		
O.ADMIN_CONTROLS - protection mechanisms to preserve the integrity of security enforcing functions	T.ADMIN_ERRORS (partial)		

Table B.1.2: Correlating TOE security objectives to threats, policies and usage assumptions

TOE Security Objective	Threat Addressed	Policy Supported	Usage Assumption
O.OVERFLOW_ ALARMS - overflow situations (in buffers, audit trails etc) present a source of security vulnerability for TOE as well result in denial of service. Hence threshold values must be designated for buffers, audit trail volumes etc., and suitable alarms must be generated when those values are reached during the course of TOE operation.	T.OVERFLOW _ERRORS	P.AVAILABILITY (partial)	

Table B.1.2 (contd..): Correlating TOE security objectives to threats, policies and usage assumptions

From an examination of the tables B.1.1 and B.1.2, it is clear that each security objective counters at least one threat and/or supports at least one policy component. Thus, there are no unnecessary objectives. Also these mapping tables provide coverage for all threats in section 3.2 and policy components in section 3.3. Further we could see that the two threats under section 3.2.3 which are meant to be addressed jointly by TOE and its environment are found in both table B.1.1 (Environmental security objectives) and table B.1.2 (TOE security objectives).

B.2 Security Functional Requirements (SFR) Rationale

B.2.1 Suitability of Security Functional Requirements

Table B.2.1 below lists each of the security functional requirements in section 5, provides a justification for its inclusion in the ADT-PP and correlates it with the security objective(s) it is meant to satisfy.

TOE Security Functional Requirement	Security Objective satisfied
FAU_GEN.1.1, FAU_GEN.1.2 (refined) FAU_GEN.2.1 - The above requirements stipulate that there is an audit generation mechanism in place and that the records generated contain all the relevant information pertaining to user/admin action so as to hold them accountable for their actions.	O.AUDIT_SETUP

TOE Security Functional Requirement	Security Objective satisfied
FAU_SAR.1.1, FAU_SAR.1.2 FAU_SAR.2.1 FAU_SAR.3.1 (refinement) - These requirements stipulate that audit records shall be in a format suitable for sorting and searching based on certain key parameters like date/time of the event, the user that caused the event, type of event etc., - Also the restrictions on access to the audit records	O.AUDIT_ SETUP, O.ADMIN_DATA _PROTECTION
FAU_SEL.1.1 (refinement), FAU_SEL.1.1-ADT.1 (extension), FAU_SEL.1.1-ADT.2 (extension) - these requirements are needed to ensure a degree of flexibility and control in the audit records generation process – i.e., to include or exclude certain auditable events as well to exercise this control process any time during TOE operation and to restrict this right to explicitly authorized administrative roles.	O.AUDIT_ SETUP, O.ADMIN_ CONTROLS
FAU_STG.1.1, FAU_STG.1.2, FAU_STG.1.3 - these requirements are in place to ensure the integrity of the stored audit records – by controlling their deletion and modification as well as to ensure uninterrupted storage operation by setting up suitable alarms when the physical storage volumes exceed a designated threshold amount.	O.AUDIT_ SETUP, O.OVERFLOW_ ALARMS
FDP_ACC.1.1 - this requirement stipulates all the entities (subjects, objects and operations) that come under the TOE access control policy	O.PRIV_SCOPE
FDP_ACF.1.1, FDP_ACF.1.2 - these requirements cover the rules governing the control of access under the TOE access control policy.	O.ROLE_SETUP, O.APPLICATION _CONTROLS
FDP_ETC.1.1, FDP_ETC.1.2 - these requirements stipulate that TOE access control policy functions should get invoked when exporting data that is within the scope of TOE access control policy to an external system.	O.PRIV_SCOPE, O.APPLICATION _CONTROLS
FDP_ITC.1.1,FDP_ITC.1.2, FDP_ITC.1.3 - these requirements stipulate that TOE access control policy functions should get invoked when importing data that is within the scope of TOE access control policy from an external system.	O.PRIV_SCOPE, O.APPLICATION _CONTROLS
FDP_UCT.1.1 - these requirements stipulate that the actual operations of transmitting and receiving data to and into TOE from external systems should also be governed by the TOE access control policy.	O.APPLICATION _CONTROLS

TOE Security Functional Requirement	Security Objective satisfied
FIA_AFL.1.1 - The number of authentication violations that the system can tolerate Must be restricted. This is necessary to distinguish between inadvertent errors in providing the right authentication data by valid users and the attempts by unauthorized users for gaining entry into the ADT system	O.OVERFLOW_ ALARMS
FIA_ATD.1.1 - The authentication and authorization process that is going to used in the TOE dictates the type of security attributes. In ADT, the authentication is based on UserIDs and authorization is based on user's assigned roles and hence at the minimum, the security attributes - User Identifier and Group/Role memberships must be maintained by the system.	O.ROLE_ SETUP
FIA_SOS.1.1, FIA_SOS.2.1 - The type of authentication mechanism used in the TOE determines the types of secrets and these requirements specify the metrics (e.g., for passwords the minimum length and type of characters allowed) for each type of secret.	O.AUTHENTICA TION_SETUP
FIA_UAU.2.1, FIA_UAU.5.1,FIA_UAU.6.1 - these requirements state the different types of authentication the TOE should support, the timing of the authentication as well under what conditions the user must be re-authenticated.	O.AUTHENTICA TION_SETUP
FIA_UID.2.1 - this requirement stipulates the timing for the user identification process.	O.AUTHENTICA TION_SETUP
FMT_MOF - the overall security of TOE depends upon the way security functions have been configured and hence modifying the behavior of these functions should be the exclusive right of a few trusted administrators.	O.ADMIN_ CONTROLS
FMT_MSA.1.1, FMT_MSA.3.1 - for a given configuration of security functions, the actual outcomes of these function operations depend upon security attributes and TOE security function data (TSF data). Hence security attributes that are applicable to the TOE under consideration must be explicitly specified and access to those must be restricted.	O.ADMIN_DATA _CONTROLS
FDP_MTD.1.1 - for a given configuration of security functions, the actual outcomes of these function operations depend upon security attributes and TOE security function data (TSF data). Hence TSF data that are applicable to TOE under consideration must be explicitly specified and access to them must be restricted.	O.ADMIN_DATA _CONTROLS
FMT_SAE.1.1, FMT_SAE.1.2 - to lessen the risk of security attributes being guessed or hacked, it is necessary to specify an expiration time for a selected subset of the overall security attributes for the TOE and to determine the follow-up actions that need to be taken just prior and/or after the expiration.	O.ADMIN_DATA _PROTECTION
FMT_SMR.1.1 - the right to perform TOE administrative operations that have security implications should be restricted to a few trusted administrators. Hence it is necessary to define a set of administrative roles for the TOE so as to channel these rights only through them.	O.ADMIN_DATA _CONTROLS

TOE Security Functional Requirement	**Security Objective satisfied**
FPT_STM.1.1 - the correct operation of many security functions depend upon the reliable generation of timestamps and TSF should incorporate this function as well.	O.APPLICATION _CONTROLS
FTA_SSL.1.1, FTA_SSL.1.1-ADT.1(extension) - session management functions play an important role in the overall security behavior of the TOE just like other functions relating to authentication, access control etc., Hence important aspects of this function must be specified (e.g., session initiation procedures, session time-out/locking etc.,)	O.ADMIN_ CONROLS
FTA_ITC.1.1 - Information under the control of ADT should be transferred in a secure way to any another remote trusted product and for this there should be the capability to set up trusted channels.	O.APPLICATION _CONTROLS

Table B.2.1 – Correlating TOE Security Functional Requirements to Security Objectives

From an examination of the tables B.2.1, it is clear that each security functional requirement satisfies at least one security objective. Thus, there are no unnecessary security functional requirements. Also the mapping table reveals that all security objectives in section 2 have been covered by the list of security functional requirements. It is generally the case that multiple security functional requirements are needed to satisfy a single security objective.

B.2.2 Security Functional Requirements Dependency Analysis

When a security functional requirement component is included in a PP, its corresponding dependent components (identified in CC) also should have been included in the PP as well. The process of verification of this property is called "Dependency Analysis" and is required to ensure that the overall set of security functional requirements are consistent and hence realizable in TOE implementation.

The following table (Table B.2.2.1) lists all the security functional requirements (SFR) components included in the ADT PP with a numeric line number. The dependencies of each component, if any, are listed alongside that component with a reference to the line number of the component that satisfies them. In cases where the dependent component is a "security assurance requirement (SAR) component" instead of an SFR component, the Reference Line column simply gives the chosen EAL level (i.e., EAL2). Reference Line numbers followed by (H) indicate that the dependency is satisfied by a hierarchical component to that referenced.

Line Number	SFR Component	Dependencies	Reference Line
1	FAU_GEN.1	FPT_STM.1	27
2	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	1 21 (H)
3	FAU_SAR.1	FAU_GEN.1	1
4	FAU_SAR.2	FAU_SAR.1	3
5	FAU_SAR.3	FAU_SAR.1	3
6	FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	1 24
7	FAU_STG.1	FAU_GEN.1	1
8	FAU_STG.3	FAU_STG.1	7
9	FDP_ACC.1	FDP_ACF.1	10
10	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	9 24
11	FDP_ETC.1	FDP_ACC.1	9
12	FDP_ITC.1	FDP_ACC.1 FMT_MSA.3	9 24
13	FDP_UCT.1	FTP_ITC.1 FDP_ACC.1	30 9
14	FIA_AFL.1	FIA_UAU.1	18(H)
15	FIA_ATD.1	-	-
16	FIA_SOS.1	-	-
17	FIA_SOS.2	-	-
18	FIA_UAU.2	FIA_UID.1	21(H)
19	FIA_UAU.5	-	-
20	FIA_UAU.6	-	-
21	FIA_UID.2	-	-
22	FMT_MOF.1	FMT_SMR.1	27
23	FMT_MSA.1	FDP_ACC.1 FMT_SMR.1	9 27
24	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	23 27
25	FMT_MTD.1	FMT_SMR.1	-
26	FMT_SAE.1	FMT_SMR.1 FPT_STM.1	27 28
27	FMT_SMR.1	FIA_UID.1	21(H)
28	FPT_STM.1	-	-
29	FTA_SSL.1	FIA_UAU.1	18(H)
30	FTP_ITC.1	-	-

Appendix C

Coverage of HIPPA Security Requirements by ADT-PP SFRs

HIPPA Security Requirement – Scope **(Explanation of Implementation Features specified in ADT PP)**	**Covering ADT-PP Security Functional Requirement**
Audit Controls – Mechanism to record System Activity (ADT PP stipulates requirements for presence of audit record generating functions and the system event parameters that should be captured in an audit record)	FAU_GEN.1.1, FAU_GEN.1.2 (refined) FAU_GEN.2.1
Audit Controls – Mechanism to examine System Activity (To examine a system activity one should be able to sort and search audit logs based on different parameters).	FAU_SAR.1.1, FAU_SAR.1.2 FAU_SAR.2.1 (restrict audit record review capability to a few ADT administrative roles) FAU_SAR.3.1 (refinement) (search, sort and order audit records for obtaining different views of system events)
Audit Controls – should enable an organization to detect suspect data access activities, assess its security programs and respond to potential weakness (to achieve multiple objectives like these, audit generation process should be flexible and easily configurable).	FAU_SEL.1.1 (refinement), FAU_SEL.1.1-ADT.1 (extension), FAU_SEL.1.1-ADT.2 (extension) (select auditable events based on different system event parameter values)
Audit Controls – High Integrity mechanism (this is an implicit HIPPA requirement – hence the system should provide secure permanent storage for audit records. Also the system should prevent and detect modifications to audit records and limit the ability to read and archive these records to a few trusted ADT administrative roles).	FAU_STG.1.1, FAU_STG.1.2, FAU_STG.1.3 (ensure secure storage for audit records) FMT_MTD.1.1 (ensure access to audit record access for all administrative purposes – archiving etc to a few ADT administrative roles).

***HIPPA Security Requirement – Scope* (Explanation of Implementation Features specified in ADT PP)**	**Covering ADT-PP Security Functional Requirement**
Access Control - ...limit access to health information to those employees who have a business need to access it (Assign all access privileges needed for a business process to a specific role and assign that role to employees based on their organizational role. Design Access Control function to enforce access restriction based on role memberships)	FDP_ACF.1.1, FDP_ACF.1.2 (Access Enforcement Rules)
Access Control – should cover all individually identifiable health information (Implict HIPPA requirement – hence access control should cover all data not only stored in ADT but also those that are imported into and exported from ADT to other related systems. Also the access control policy should stipulate whether data export and/or import should or should not be associated with security attributes	FDP_ETC.1.1, FDP_ETC.1.2 (Access Control for Exported Data) FDP_ITC.1.1,FDP_ITC.1.2, FDP_ITC.1.3 (Access Control for Imported Data)
Authorization Controls - ...necessary to ensure that health information is used only by properly authorized individuals (Proper Authorization can be ensured by limiting the ability to alter the security attributes like User IDs and Role Memberships (from which the access privileges flow) to a few trusted ADT administrative roles).	FMT_MSA.1.1, FMT_MSA.3.1, FMT_MSA.3.2 (Security Attribute manipulation features available for ADT administrative roles)
Data Authentication – Data Corroboration may be assured .. through the use of checksum, double keying, a message authentication code or digital signature (Since all the data that ADT deals with – either native to ADT or imported from other systems are created by authorized persons through proper access controls, no authentication is required except for use of time stamps for verification)	FPT_STM.1.1 (Time Stamps)

HIPPA Security Requirement – Scope **(Explanation of Implementation Features specified in ADT PP)**	**Covering ADT-PP Security Functional Requirement**
Entity Authentication – Unique User Identification (The system should provide ability to create Unique User Identifiers to a few trusted ADT administrators as well to activate/deactivate those identifiers and specify expiration time for those identifiers)	FIA_UID.2.1, FIA_ATD.1.1 (Create, Maintain User Identifiers, User Identification Mechanism) FMT_MOF.1.1 (User Identifiers Activation/Deactivation function) FMT_SAE.1.1, FMT_SAE.1.2 (Specification of Expiry Time for User IDs)
Entity Authentication – .. at least one of the following implementation features would be used: A biometric identification system, A password system, A personal identification number, Telephone callback, A token system which uses a physical device for user identification (ADT PP not stipulates Passwords and/or Smart Tokens/Cards but also requires these authentication schemes to meet a quality metric).	FIA_UAU.2.1, FIA_UAU.5.1 (Authentication mechanisms) FIA_SOS.1.1, FIA_SOS.2.1 (metrics for various authentication mechanisms)
Entity Authentication – Enhanced Authentication Integrity (this is an implied HIPAA requirement. To meet this objective ADT PP stipulates conditions under which re-authentication is required, measures to deal with authentication failure and specification of expiration time for User Passwords and/or tokens).	FIA_UAU.6.1 (re-authentication conditions) FIA_AFL.1.1, FIA_AFL.1.2 (authentication-failure handling) FIA_SAE.1.1, FIA_SAE.1.2 (specification of expiry time for authentication data)
Entity Authentication – the following implementation feature should be used: Automatic log off (ADT PP not only stipulates termination of user session after a specific period of inactivity but also re-authentication conditions for interfaces like web browsers where session protocol semantics are not defined).	FTA_SSL.3.1 (conditions for session termination and re-authentication for stateless interactions)

HIPPA Security Requirement – Scope **(Explanation of Implementation Features specified in ADT PP)**	**Covering ADT-PP Security Functional Requirement**
Technical Security Mechanisms to Guard Against Unauthorized Access to Data That is Transmitted Over a Communications Network – One of the following implementation features should be in place: Access Controls, Encryption (ADT PP stipulates that data transfer process itself (both transmit and receive) should be subject to access controls (limiting the set of users who can exchange data as well the types of data that can be exchanged) and the process should be done in a confidential manner and the data in transit should be protected from modification or disclosure by establishing a protected communication channel)	FDP_UCT.1.1 (Data Transfer Confidentiality) FTP_ITC.1.1, FTP_ITC.1.2, FTP_ITC.1.3 (Establishment of and Functionality required for Trusted Channel)

Appendix D

Bibliography

[1] A Methodology for Development of Security Architectures for Healthcare Information Systems- Ramaswamy Chandramouli & Arnold Johnson –under Review to be published as a NIST Special Publication.

[2] Draft HIPAA Security Summit Guidelines – January 12, 2000

[3] Forum on Privacy and Security in Healthcare, http://www.healthcaresecurity.org/

[4] ISO/IEC International Standard (IS) 15408, Parts 1 thru 3 at http://csrc.nist.gov/cc/ccv20/ccv2list.htm

[5] NIAP CC Evaluation and Validation Scheme, http://niap.nist.gov/cc-scheme/index.html

[6] Security and Electronic Signature Standards; Proposed Rule, Federal Register/Vol 63, No. 155, Aug 12, 1998.